Barracuda SSL VPN - *Quick Start Guide*

The Barracuda SSL VPN provides remote users secure, clientless access to their internal network. The Barracuda SSL VPN may be installed directly inside the LAN or in a more complex DMZ configuration.

1 Getting Started

Follow the instructions in this guide to configure the Barracuda SSL VPN to accept incoming connections from the Internet. To begin setting up your Barracuda SSL VPN, you will need the following:

- Barracuda SSL VPN
- AC Power Cord
- Ethernet Cables
- VGA Monitor (recommended)
- PS2 Keyboard (recommended)

2 Physical Installation

To install the Barracuda SSL VPN:

1. Fasten the Barracuda SSL VPN to a 19-inch rack or place it in a stable location.
2. Connect an Ethernet cable from your network switch to the Ethernet port on the back of the Barracuda SSL VPN.
3. Connect a VGA Monitor, PS2 Keyboard, and AC power cord to the unit.
4. Press the power button on the front panel to turn the unit on.

3 Configure IP Address and Network Settings

If you have a monitor connected, the Barracuda SSL VPN will display the Boot Menu initially, and the Administrative Console login prompt once fully booted. To begin the configuration:

1. Login to the Administrative Console using the admin login:
   - **Login**: `admin`
   - **Password**: `admin`

2. Configure the **IP Address, Subnet Mask, Default Gateway, Primary DNS Server** and **Secondary DNS Server** as appropriate for your network.

If you do not have a monitor and keyboard and want to set the IP address using the RESET button on the front panel, press and hold the RESET per the following table:

IP address	**Press and hold RESET for**…
192.168.200.200	5 seconds
192.168.1.200	8 seconds
10.1.1.200	12 seconds

4 Open Firewall Ports

If your Barracuda SSL VPN is located behind a corporate firewall, open the following ports on your external firewall to ensure proper operation:

Port	**Direction**	**TCP**	**UDP**	**Usage**
22	Out	Yes	No	Remote diagnostics and service (recommended)
25	Out	Yes	No	Email alerts + One-time passwords
53	Out	Yes	Yes	Domain Name Service (DNS)
80	Out	Yes	No	Firmware and definition updates
123	Out	No	Yes	Network Time Protocol (NTP)
443	In	Yes	No	HTTPS/SSL port for SSL VPN access
8000	Out	Yes	No	Firmware and definition updates (backup)
8000	In*	Yes	No	External appliance administrator port (HTTP)*
8443	In*	Yes	No	External appliance administrator port (HTTPS)*

** Only if appliance management is performed from outside the corporate network*

The following ports must be opened if the listed type of access is desired:

1723	In	Yes	No	**PPTP** access**
500	In	No	Yes	**L2TP/IPsec** access
4500	In	No	Yes	**L2TP/IPsec** access

*** Note: **PPTP** access also requires GRE (IP protocol 47)*

If you also have an internal firewall (due to placing the Barracuda SSL VPN in a DMZ, for example), then the following must be allowed on your internal firewall:

389	Out	Yes	No	LDAP/Active Directory read access
636	Out	Yes	No	LDAP/Active Directory read/write access

5 Barracuda SSL VPN Configuration

Use a computer with a Web browser that is connected to the same network as the Barracuda SSL VPN and follow these steps:

1. In your web browser's address bar, enter http:// followed by the IP address of the Barracuda SSL VPN, followed by the default Appliance Administrator web interface HTTP port (:8000). For example, if you configured the Barracuda SSL VPN with an IP address of 192.168.200.200, you would type:
   `http://192.168.200.200:8000`
2. Log in to the Appliance Administrator web interface as the administrator:
   Username: `admin` **Password:** `admin`
3. Go to the **BASIC > IP Configuration** page and perform the following:
   - Verify the **IP Address**, **Subnet Mask**, and **Default Gateway**.
   - Verify the **Primary** and **Secondary DNS Server**.
   - Enter the **Default Hostname** and **Default Domain**.
   - If you are using a proxy server on your network, you should also verify the **Proxy Server Configuration** settings.
4. Complete the rest of the fields on this page and save your changes.

Barracuda SSL VPN - *Quick Start Guide*

6 Activate Subscriptions

Verify that the Energize Updates feature is activated on your Barracuda SSL VPN – this is required to enable further configuration.

1. Go to the **Basic > Status** page.
2. Under Subscription Status, if **Energize Updates** is **Not Activated**, click the activation link to be redirected to the Barracuda Networks Product Activation page. Complete activation of your subscription(s).

If it is connected to the Internet, the Barracuda SSL VPN automatically updates its activation status after you reload the browser page when viewing the **Basic > Status** page.

7 Update the Firmware

Go to the **ADVANCED > Firmware Update** page. If there is a new **Latest General Release** available, perform the following steps to update the system firmware:

1. Click the **Download Now** button located next to the Latest General Release firmware version. To view the progress of the download progress, click **Refresh**. To avoid damaging the Barracuda SSL VPN, do not power off the system during an update or download
2. When the download is complete, click **Apply Now** to apply the firmware. Click **OK** to acknowledge the reboot message. Applying the firmware takes a few minutes to complete.
3. After applying the firmware, the Barracuda SSL VPN will automatically reboot. When the system comes back up, the login page is displayed. Log in again.

8 Change the Administrator Password

To avoid unauthorized use, we recommend you change the password for the default Appliance Administrator web interface to a more secure password.

1. Go to **BASIC > Administration** to change your password.
2. Complete the rest of the fields on this page.

9 Route Incoming SSL Connections to the Barracuda SSL VPN

To take advantage of all available features, you must route HTTPS incoming connections on port 443 to the Barracuda SSL VPN. This is typically achieved by configuring your corporate firewall to port forward SSL connections directly to the Barracuda SSL VPN.

Note: The Appliance Administrator web interface ports on 8000/8443 will also need similar port forward configurations if you intend to manage the appliance from outside the corporate network.

10 Verify Incoming Connections to the Barracuda SSL VPN

Once you have configured your corporate firewall to route SSL through to the Barracuda SSL VPN, you should be able to accept incoming SSL connections.

1. To test the connection, use a web browser from the Internet (not inside the LAN) to establish an SSL connection to the external IP address of your corporate firewall. For example, if your firewall's external IP address is 192.168.1.1, direct your browser to: `https://192.168.1.1`
2. If you receive a warning in your browser about an untrusted SSL certificate, accept the warning to load the page.
3. On the login page for the SSL VPN interface, log in with the credentials for the VPN administrator:
   Username: `ssladmin` **Password:** `ssladmin`
4. You will now be successfully logged in as the VPN administrator, and taken directly to the SSL VPN Management Interface. From here you can set up accounts and other resources for users of the Barracuda SSL VPN.

11 Additional Post-Setup Configuration Items

Your Barracuda SSL VPN should now be able to accept incoming connections from the Internet. However, the following ***additional steps*** should be performed to fully complete the initial configuration:

- Register a hostname with your DNS server for the Barracuda SSL VPN, such as: *sslvpn.example.com*
- Install an SSL certificate on the Barracuda SSL VPN for the hostname, to ensure your users can confirm that they are connecting to a genuine Barracuda SSL VPN that is registered to your organization.
- Integrate the Barracuda SSL VPN with your existing user database. To cleanly integrate with your environment, the Barracuda SSL VPN can read in user accounts and authenticate against a number of different databases, including Microsoft Active Directory and LDAP.
- Grant users access to resources using the policy framework. Create a number of policies that best represent your organization's structure and then link resources and users. Users that are not part of the policy are denied access while those that are part of the policy are allowed access to these resources.
- Further refine your access policies by managing user access rights. If your network uses a DMZ, you may wish to configure the Barracuda SSL VPN in this topology for greater security.

Additional documentation, including the Barracuda SSL VPN Administrator's Guide, can be found at **http://www.barracuda.com/documentation**.

Contact and Copyright Information
Barracuda Networks, Inc. 3175 S. Winchester Blvd, Campbell, CA 95008 USA • phone: 408.342.5400 • fax: 408.342.1061 • www.barracuda.com
Copyright 2004-2012 © Barracuda Networks, Inc. All rights reserved. Use of this product and this manual is subject to license. Information in this document is subject to change without notice. Barracuda SSL VPN is a trademark of Barracuda Networks, Inc. All other brand and product names mentioned in this document are registered trademarks or trademarks of their respective holders. 21-120118-mb